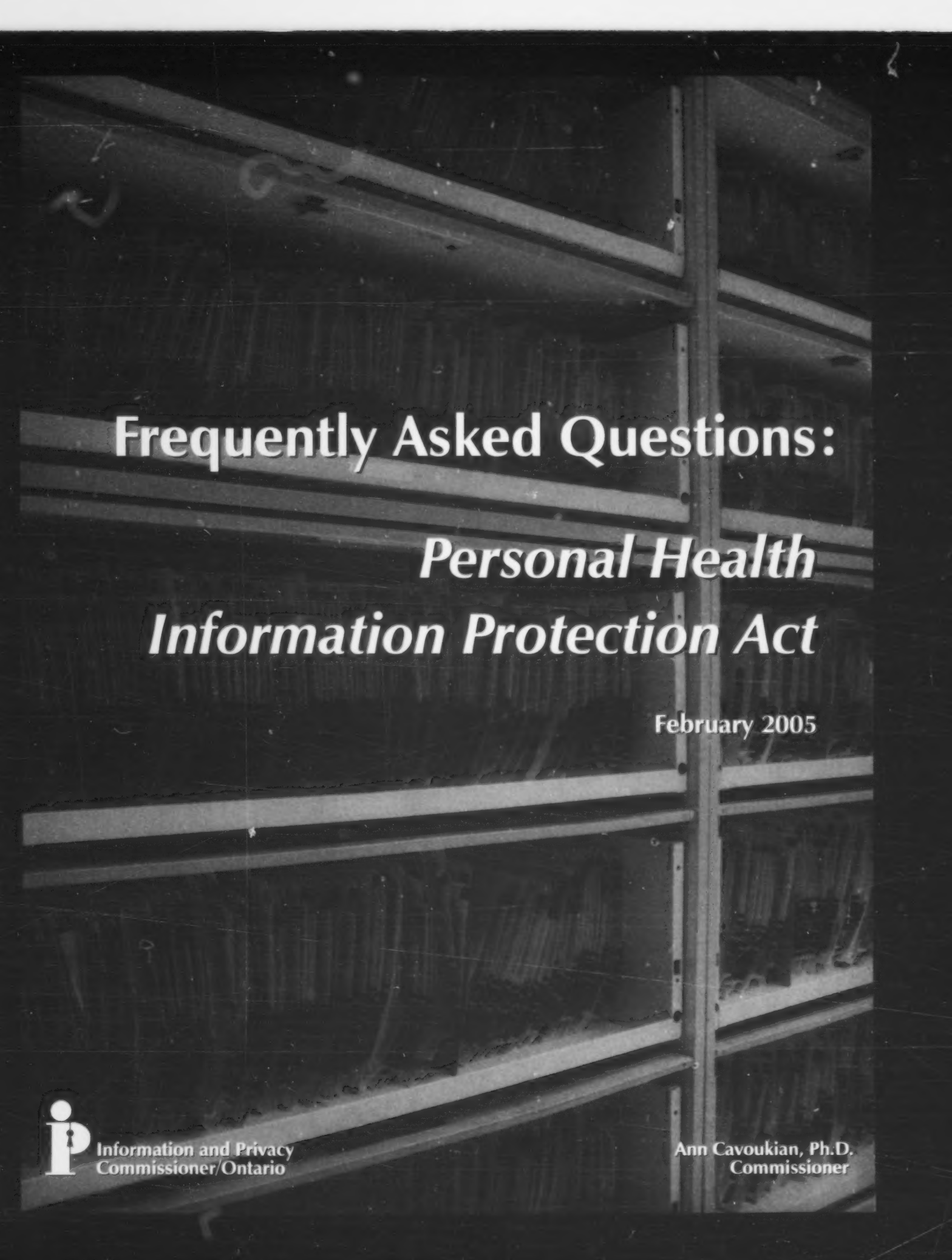

Frequently Asked Questions:

Personal Health Information Protection Act

February 2005

Information and Privacy Commissioner/Ontario

Ann Cavoukian, Ph.D.
Commissioner

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Sylvia Klasovec and Mark Ratner in preparing this document.

This FAQ provides a general overview of the *Personal Health Information Protection Act, 2004*, S.O. 2004, c.3. and *Regulation 329/04*. The information contained in this document is for general reference purposes only and should not be construed as legal advice. You should consult with your own solicitor for all purposes of interpretation.

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Background 1

Introduction 2

What is the *Personal Health Information Protection Act, 2004* (*PHIPA*)? 2

When did *PHIPA* come into force? 2

Is *PHIPA* retroactive? 3

Overview 4

What is the purpose of *PHIPA*? 4

Why do we need a health privacy law in Ontario? 4

What is the relationship between *PHIPA* and the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)? 5

Application and Scope of *PHIPA* 6

To whom does *PHIPA* apply? 6

Does *PHIPA* apply to insurance companies or employers? 6

What is a health information custodian? 6

What is an agent? 7

What is the 'circle of care?' 8

What is personal health information? 8

What does 'health care' mean? 9

What is a prescribed registry? 9

What is a prescribed entity? 10

What is a health information network provider? 11

Rights and Responsibilities 12

How does *PHIPA* protect personal health information? 12

What rights do individuals have? 12

What responsibilities do health information custodians have? 13

What is the responsibility of a health information custodian who works for a non-health information custodian? 14

Consent Requirements 15

What is consent under *PHIPA*? 15

What is the difference between express and implied consent? 15

What are the requirements for consent? 15

When is implied consent sufficient? 16

When is express consent required? 16

Are pharmacists required to obtain express consent from an individual to disclose personal health information to a third party benefits payor? 17

Can an individual withdraw his/her consent? 17

Can an individual control what personal health information is recorded in his/her file? 17

What is a 'lock-box?' 17

How does the lock-box work? 18

When does the lock-box provision take effect? 18

What happens when an individual is incapable of providing consent? 18

Can another person, such as a family member, provide consent on an individual's behalf when picking up or dropping off a prescription? 19

Collection, Use and Disclosure of Personal Health Information 20

Collection 20

Use 21

Disclosure 22

What is a health data institute? 25

Can a health information custodian disclose personal health information to the Workplace Safety and Insurance Board (WSIB) about an injured worker without the individual's consent? 25

Fundraising and Marketing 26

Can health information custodians collect, use or disclose personal health information for fundraising activities? 26

Can personal health information be collected, used or disclosed for marketing purposes? 26

Research 27

What are the requirements for the collection, use and disclosure of personal health information for health care research? 27

Are there any requirements for research ethics boards and research plans? 28

Ontario Health Cards and Health Numbers 29

Who can collect, use or disclose Ontario health card numbers and under what circumstances may this be disclosed? 29

Are other organizations permitted to request the production of a health card? 29

Access to Personal Health Information 31

Are individuals permitted to access their own personal health information? 31

How does an individual obtain access to his/her personal health information? 31

How long does a health information custodian have to respond to an individual's request for access to personal health information? 31

Can a health information custodian refuse to provide access to an individual's personal health information? 32

Is there a fee associated with an access request? 32

Can an individual obtain access to his/her personal health information from a health information custodian who works for a non-health information custodian? 32

What if the health information custodian works for a non-health information custodian that is covered under public sector access and privacy legislation, such as a school board or municipality? 33

Corrections to Personal Health Information 34

Can an individual correct errors in his/her personal health information? 34

How does an individual correct errors? 34

Can a health information custodian refuse to correct an individual's personal health information? 34

Administration and Enforcement 35

How will *PHIPA* be enforced? 35

How does an individual initiate a complaint? 35

Is there a time limit within which an individual may complain? 36

If an individual is not satisfied with an IPC order, what can be done? 36

What are the consequences for committing an offence under *PHIPA*? 36

What is an offence under *PHIPA*? 37

The *Quality of Care Information Protection Act, 2004* 38

What is the *Quality of Care Information Protection Act, 2004* (*QOCIPA*)? 38

Background

The *Health Information Protection Act, 2004* was introduced in the Legislature on December 17, 2003 and received Royal Assent on May 20, 2004.

The legislation contains two schedules: the *Personal Health Information Protection Act, 2004* (Schedule A) and the *Quality of Care Information Protection Act, 2004* (Schedule B). Together, these schedules comprise the *Health Information Protection Act, 2004.*

This FAQ will address the *Personal Health Information Protection Act, 2004* (*PHIPA*).

Introduction

What is the *Personal Health Information Protection Act, 2004* (*PHIPA*)?

The *Personal Health Information Protection Act, 2004* (*PHIPA*) is Ontario's new health-specific privacy legislation. *PHIPA* governs the manner in which personal health information may be collected, used and disclosed within the health care system. It also regulates individuals and organizations that receive personal information from health care professionals.

PHIPA creates a consistent approach to protecting personal health information across the health care system. By providing a level playing field for all health care professions, *PHIPA* builds upon and codifies many of the existing high standards and protections enshrined in the common law, various professional codes, policies and guidelines.

These legislated rules were designed to give individuals greater control over how their personal health information is collected, used or disclosed. They provide health care professionals with a flexible framework to access and use health information as necessary in order to deliver adequate and timely health care.

In addition, *PHIPA* confirms a patient's existing right to access one's own personal health information and provides a means for redress through the Office of the Information and Privacy Commissioner/Ontario (IPC) when privacy rights relating to personal health information have been violated.

The IPC has been designated as the oversight body responsible for administering and enforcing these new health sector privacy rules. As such, we have prepared the following questions and answers to guide Ontarians and health care professionals in understanding their respective privacy rights and obligations.

When did *PHIPA* come into force?

PHIPA came into force on November 1, 2004. As of that date, all health information custodians and recipients of personal health information must comply.

Is *PHIPA* retroactive?

No. *PHIPA* applies to the collection, use and disclosure of personal health information by health information custodians as of November 1, 2004. There is no obligation for custodians to seek consent for personal health information that was collected prior to this date. However, a health information custodian must obtain consent for the use or disclosure of that information after November 1.

In addition, as of November 1, 2004, *PHIPA* will apply to the use and disclosure of personal health information by any person who is not a health information custodian and who has received the information from a custodian, before or after this date.

Overview

What is the purpose of *PHIPA*?

PHIPA establishes a set of uniform rules about the manner in which personal health information may be collected, used or disclosed, and includes provisions that:

- Require consent for the collection, use and disclosure of personal health information, with necessary but limited exceptions;
- Require that health information custodians treat all personal health information as confidential and keep it secure;
- Strengthen an individual's right to access his/her personal health information, as well as the right to correct errors;
- Give a patient the right to instruct health information custodians not to share any part of his/her personal health information with other health care providers;
- Establish clear rules for the use of personal health information for fundraising or marketing purposes;
- Set guidelines for the use and disclosure of personal health information for research purposes;
- Ensure accountability by granting an individual the right to complain to the IPC about the practices of a health information custodian; and
- Establish remedies for breaches of the legislation.

Why do we need a health privacy law in Ontario?

Personal health information is among the most sensitive of personal information. People are understandably protective about sharing personal details relating to their medical conditions. At the same time, personal health information must flow freely between health care professionals in order to ensure the best treatment for patients.

The nature of our health care system is that health information passes through many links in the health care chain: from a doctor's office, to a referral to a specialist, to a medical lab, to a hospital or to an insurance company for reimbursement of claims. There are also circumstances in which personal health information must be readily shared, such as in the case

of a medical emergency. Beyond patient care, personal health information is needed for important activities such as health research vital to develop new treatments and cures. The increasing use of technology to transfer and store medical data instantaneously has also increased the need for legislated rules to assure Ontarians that their personal health information will be strongly protected.

What is the relationship between *PHIPA* and the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)?

The collection, use and disclosure of personal information within the commercial sector is regulated by federal privacy legislation — the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). *PIPEDA* was enacted to regulate the collection, use or disclosure of personal information in the hands of private sector organizations. As of January 1, 2004, *PIPEDA* has applied to all Ontario private sector organizations, including pharmacies, laboratories, and health care providers with operating practices that qualify as "commercial activities." *PIPEDA* does not apply to personal information in provinces and territories that have "substantially similar" privacy legislation in place.

The application of *PIPEDA* to personal health information has raised a number of concerns. The requirements under *PIPEDA* were designed to regulate direct marketing, electronic commerce and other analogous activities and do not specifically address the unique circumstances encountered within the health care system. The federal government is expected to deem the provisions of Ontario's *PHIPA* to be substantially similar to *PIPEDA* in order to exempt health care providers that are covered under *PHIPA* from also having to comply with the provisions of *PIPEDA*.

However, even if such an exemption is made, *PIPEDA* will continue to apply to all commercial activities relating to the exchange of personal health information between provinces and territories and to information transfers outside of Canada.

Application and Scope of *PHIPA*

To whom does *PHIPA* apply?

PHIPA applies to a wide variety of individuals and organizations defined as health information custodians. *PHIPA* also applies to agents who are authorized to act for or on behalf of a health information custodian.

Does *PHIPA* apply to insurance companies or employers?

Certain organizations, such as insurance companies and employers, who may hold personal health information in their files are not governed by *PHIPA* unless they receive personal health information from a health information custodian. When an insurance company or employer receives personal health information from a custodian, the receiving entity may, in general, only use or disclose the information for the authorized purpose for which the information was received or for the purpose of carrying out a statutory or legal duty. This rule is coloquially referred to as the "recipient rule."

However, an exception to the recipient rule applies to insurance providers that receive personal health information from a pharmacist. In that situation, *PHIPA* permits the insurance provider to disclose personal health information to the pharmacist to assist the pharmacist in advising the individual or providing the individual with health care. For example, the insurer may disclose to a pharmacist the types of medications an individual has purchased from different pharmacies so that the pharmacist may advise of any incompatible prescriptions.

What is a health information custodian?

A health information custodian is a listed individual or organization under *PHIPA* that, as a result of his or its power or duties, has custody or control of personal health information. Examples of health information custodians include:

- Health care practitioners, (including doctors, nurses, audiologists and speech-language pathologists, chiropractors, chiropodists, dental professionals, dieticians, medical radiation technologists, medical laboratory technologists, massage therapists, midwives, optometrists, occupational therapists, opticians, pharmacists, physiotherapists, psychologists and respiratory therapists);
- Hospitals;
- Psychiatric facilities;
- Pharmacies;

- Laboratories;
- Nursing homes and long-term care facilities;
- Homes for the aged and homes for special care;
- Community care access corporations;
- Ambulance services;
- Boards of health;
- The Minister of Health and Long-Term Care; and
- The Canadian Blood Services.

A health information custodian does not include:

- An aboriginal healer or aboriginal midwife who provides traditional healing services to aboriginal persons or members of an aboriginal community; and
- A person who provides treatment by spiritual means or by prayer.

What is an agent?

PHIPA defines an agent to include any person who is authorized by a health information custodian to perform services or activities on the custodian's behalf and for the purposes of that custodian.

An agent may include an individual or company that contracts with, is employed by or volunteers for a health information custodian and, as a result, may have access to personal health information. *PHIPA* permits custodians to provide personal health information to their agents only if the custodian is permitted to collect, use, disclose, retain or dispose of the information.

For example, an agency relationship under *PHIPA* includes a nurse who is employed by, or a medical student who volunteers at, a hospital. An agency relationship may also include a physician who is not employed by a hospital but has admitting privileges to use the hospital's equipment or facilities.

In such cases, the custodian hospital is permitted to authorize the agent to handle or deal with personal health information on its behalf so long as the agent complies with *PHIPA* and adopts the information practices of the custodian.

What is the 'circle of care?'

The "circle of care" is not a defined term under *PHIPA*. It is a term of reference used to describe health information custodians and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing or handling personal health information for the purpose of providing direct health care.

For example,

- In a physician's office, the circle of care includes: the physician, the nurse, a specialist or other health care provider referred by the physician and any other health care professional selected by the patient, such as a pharmacist or physiotherapist;
- In a hospital, the circle of care includes: the attending physician and the health care team (e.g., residents, nurses, technicians, clinical clerks and employees assigned to the patient) who have direct responsibilities of providing care to the individual.

The circle of care does not include:

- A physician who is not part of the direct or follow-up treatment of an individual;
- A medical officer of health or a board of health;
- An evaluator under the *Health Care Consent Act, 1996*;
- An assessor under the *Substitute Decisions Act, 1992*; and
- The Minister, together with the Ministry of Health and Long-Term Care.

What is personal health information?

Personal health information is "identifying information" collected about an individual, whether oral or recorded. It includes information about an individual's health or health care history in relation to:

- The individual's physical or mental condition, including family medical history;
- The provision of health care to the individual;
- Long-term health care services;
- The individual's health card number;

- Blood or body-part donations;
- Payment or eligibility for health care; and
- The identity of a health care provider or a substitute decision-maker for the individual.

"Identifying information" includes health information that could identify an individual when used alone or in conjunction with other information.

Personal health information does not include identifying information about an employee or agent of the custodian that is not maintained for the provision of health care. For example, a doctor's note to support an absence from work in the personnel file of a secretary employed by a health information custodian is not considered personal health information.

What does 'health care' mean?

"Health care" means any observation, examination, assessment, care, service or procedure provided for a health-related purpose and that is carried out or provided:

- For diagnosis, treatment or maintenance of an individual's physical or mental condition;
- For prevention of disease or injury or the promotion of health; or
- As part of palliative care.

It also includes:

- The compounding, dispensing, or selling of a drug, device or equipment pursuant to a prescription;
- A community service that is described in the *Long-Term Care Act, 1994*; and
- Taking blood or a blood product donation from an individual.

What is a prescribed registry?

The regulations prescribe a list of persons who compile and maintain registries of personal health information for the purpose of facilitating or improving the provision of health care or that relates to the storage or donation of bodily substances. Health information custodians

are permitted to disclose personal health information without consent to these listed persons. They consist of the following:

- Cardiac Care Network of Ontario in respect of its registry of cardiac services;
- INSCYTE (Information System for Cytology) in respect of its registry of CytoBase;
- London Health Sciences Centre in respect of the Ontario Joint Replacement Registry; and
- Canadian Stroke Network in respect of the Canadian Stroke Registry.

The above-noted registries may use and disclose personal health information for the purpose of facilitating or improving the provision of health care or for the storage or donation of bodily substances. They are also permitted to use and disclose personal health information for research purposes with a research plan approved by a research ethics board (REB) in certain circumstances. These persons are also permitted to disclose personal health information to prescribed entities for the planning, management or analysis of the health system.

The regulations also require that registries make publicly available:

- A plain language description of the functions of the registry; and
- Practices and procedures approved by the Commissioner to protect the security and confidentiality of the personal health information that it receives.

What is a prescribed entity?

The regulations prescribe a list of entities, including any registries maintained within these listed entities, that health information custodians are permitted to disclose personal health information to without consent for the purposes of planning and management of the health system. Prescribed entities consist of the following:

- Cancer Care Ontario (CCO);
- Canadian Institute for Health Information (CIHI);
- Institute for Clinical Evaluative Sciences (ICES); and
- Pediatric Oncology Group of Ontario (POGO).

In certain circumstances, with a research plan approved by a research ethics board, these prescribed entities are permitted to use and disclose personal health information for research purposes as if they were health information custodians. A prescribed entity is also permitted to disclose personal health information to a prescribed person who compiles or maintains a registry of personal health information, and for purposes related to the planning, management and analysis of the health care system.

These entities must make publicly available a plain language description of the functions of the entity, including a summary of the practices and procedures approved by the Commissioner for maintaining the confidentiality of the information.

What is a health information network provider?

PHIPA defines a health information network provider as a person who supplies goods and services to two or more health information custodians that enable the custodians to collect, use, modify, disclose, retain or dispose of personal health information electronically, if certain requirements are met. Health information network providers must:

- Notify the custodian of any breaches;
- Perform risk and privacy assessments;
- Provide an audit trail;
- Ensure that third parties comply with the restrictions on the use and disclosure of personal health information;
- Enter into an agreement with the custodian; and
- Make publicly available information about the provider's services to the custodian.

Rights and Responsibilities

How does *PHIPA* protect personal health information?

The ability of an individual to control how his/her own personal health information is collected, used and disclosed is key to his/her privacy rights. *PHIPA* gives patients control over their own personal health information by requiring health information custodians to obtain consent for the collection, use or disclosure of personal health information, with limited exceptions.

PHIPA establishes certain privacy rights for individuals and imposes specific obligations on health information custodians in protecting personal health information.

What rights do individuals have?

Individuals can expect to be well informed about how their personal health information will be collected, used and disclosed by health information custodians. Individuals can also expect the administrative, technical and physical safeguards relating to their personal health information to continue to be in place.

PHIPA gives individuals the right to:

- Understand the purposes for the collection, use and disclosure of personal health information;
- Refuse or give consent to the collection, use or disclosure of personal health information, except in circumstances specified in *PHIPA*;
- Withdraw consent by providing notice to the health information custodian;
- Request access to one's own personal health information;
- Request corrections to be made to one's own personal health information;
- Complain to the IPC about a custodian's refusal to give access to all or part of a health record; and
- Complain to the IPC about any breach of *PHIPA* in the manner in which personal health information has been collected, used, disclosed or handled.

PHIPA establishes a formal process for individuals to access and correct their own personal health information, within specified time frames and the right to complain if an access or correction request is denied.

What responsibilities do health information custodians have?

PHIPA requires health information custodians who have custody or control of personal health information to establish and implement information practices that comply with its provisions. This does not mean that custodians are expected to completely set aside their existing policies and practices. In fact, *PHIPA* builds upon existing policies and guidelines for health care professionals and provides enforceable rules relating to the collection, use or disclosure of personal health information.

PHIPA will require health information custodians to:

- Obtain an individual's consent when collecting, using and disclosing personal health information, except in limited circumstances as specified under *PHIPA*;
- Collect personal health information appropriately (by lawful means and for lawful purposes) and no more than is reasonably necessary;
- Take reasonable precautions to safeguard personal health information, including:
  - Protection against theft or loss;
  - Protection against unauthorized use, disclosure, copying, modification or destruction; and
  - Notification to an individual at the first reasonable opportunity if the information is stolen, lost or accessed by an unauthorized person.
- Ensure health records are as accurate, up-to-date and complete as necessary for the purposes which they use or disclose personal health information;
- Ensure health records are stored, transferred and disposed of in a secure manner;
- Designate or take on the role of a contact person who is responsible for:
  - Responding to access/correction requests;
  - Responding to inquiries about the custodian's information practices;
  - Receiving complaints regarding any alleged breaches of *PHIPA*; and
  - Ensuring overall compliance with *PHIPA*.

- Provide a written statement that is readily available to the public and describes:
    - A custodian's information practices;
    - How to reach the contact person; and
    - How an individual may obtain access, request a correction or make a complaint regarding his/her personal health information.
- Inform an individual of any uses and disclosures of personal health information without the individual's consent that occurred outside the custodian's information practices; and
- Ensure that all agents of the custodian are appropriately informed of their duties under *PHIPA*.

What is the responsibility of a health information custodian who works for a non-health information custodian?

A health care practitioner who has custody or control over personal health information but who contracts with, is employed by or volunteers for an organization that is not defined as a health information custodian under *PHIPA*, is not an agent. In such a circumstance, the individual would fall within the definition of a health information custodian under *PHIPA* and must ensure compliance.

Examples of health information custodians who work for non-health information custodians include:

- A nurse employed by a school board to provide health care services to students;
- A doctor employed by a professional sports team in order to diagnose sporting injuries;
- A registered massage therapist providing health care services to clients of a spa; and
- A nurse employed in-house by a manufacturing firm in a health care capacity.

Consent Requirements

What is consent under *PHIPA*?

The general rule is that a health information custodian needs to obtain an individual's consent to collect, use and disclose personal health information unless *PHIPA* allows the collection, use or disclosure without consent. An individual's consent may be express or implied.

What is the difference between express and implied consent?

Where consent is required under *PHIPA*, consent may be either *express* or *implied*.

Express consent to the collection, use or disclosure of personal health information by a health information custodian is explicit and direct. It may be given verbally, in writing or by electronic means.

Implied consent permits a health care custodian to infer from the surrounding circumstances that an individual would reasonably agree to the collection, use or disclosure of his/her personal health information.

For example, when an individual discloses his/her personal health information for the purposes of filling out a prescription, a pharmacist can reasonably infer consent to the collection of that information.

What are the requirements for consent?

Under *PHIPA*, consent is considered to be valid if it is:

- Knowledgeable;
- Voluntary (not obtained through deception or coercion);
- Related to the information in question; and
- Given by the individual.

Knowledgeable consent means that an individual must know why a health information custodian collects, uses or discloses his/her personal health information and that he/she may withhold or withdraw this consent.

Administratively, a health information custodian may ensure that consent is knowledgeable by posting a conspicuous notice or distributing brochures that are readily available to the public describing the purposes for the collection, use and disclosure of personal health information.

When is implied consent sufficient?

In practice, a health information custodian is not required to obtain an individual's written or verbal consent every time personal health information is collected, used or disclosed. *PHIPA* permits a custodian to assume implied consent where information is exchanged between custodians within the circle of care for the purpose of providing direct health care — unless a custodian is aware that an individual has expressly withheld or withdrawn his/her consent. Consent may never be implied for an individual who specifies that his/her personal health information may not be collected, used or disclosed.

Implied consent is also permitted if a health information custodian collects, uses or discloses names or addresses for the purposes of fundraising.

In addition, if an individual has provided information about his/her religious affiliation to a health care facility, the facility may rely on implied consent to disclose the individual's name and location within the facility to a person representing his/her religious organization. Before making this disclosure, the facility must provide the individual with an opportunity to withhold or withdraw the consent.

When is express consent required?

Subject to very limited exceptions, express consent is required:

- Where personal health information is disclosed to an individual or organization, such as an insurance company, that is not a health information custodian.
- Where information is disclosed by one custodian to another for a purpose other than providing or assisting in providing health care.
- Express consent is also required where a custodian:
    - Collects, uses or discloses personal health information other than an individual's name and mailing address for fundraising purposes;
    - Collects personal information for marketing research or activities; and
    - Collects, uses or discloses personal information for research purposes, unless certain conditions and restrictions are met.

Are pharmacists required to obtain express consent from an individual to disclose personal health information to a third party benefits payor?

No. The regulation provides an exception to the express consent requirement where a pharmacist discloses personal health information to a third party who is not a health information custodian and who is being asked to provide payment for a medication or related goods or services provided to an individual.

Pharmacists are permitted to rely on an individual's implied consent if they provide or post a notice that explains how an individual's personal health information is used and to whom it will be disclosed.

Can an individual withdraw his/her consent?

Yes. An individual may withdraw his/her consent at any time for the collection, use, or disclosure of his/her personal health information by providing notice to the health information custodian. This applies to implied as well as express consent.

A withdrawal of consent is not retroactive. This means that where a disclosure has been made on the basis of consent, the custodian is not required to retrieve the information that has already been disclosed.

Can an individual control what personal health information is recorded in his/her file?

Yes, but any condition placed on the collection, use or disclosure of personal health information cannot prohibit the recording of personal health information that is required by law, professional or institutional practice.

What is a 'lock-box?'

The "lock-box" is not a defined term under *PHIPA*. It is a term of reference used to describe the right of an individual to instruct a health information custodian not to disclose specified personal health information to another custodian for the purpose of providing health care. An individual can be said to have placed his/her personal health information into a lock-box by expressly withholding or withdrawing consent for his/her health information to be collected, used or disclosed.

How does the lock-box work?

When an individual requests a health information custodian not to use or disclose his/her personal health information to another custodian, the custodian is obliged to inform the recipient custodian that some personal health information is inaccessible as a result of it having been "locked" by the individual, if the custodian considers some of the locked information to be reasonably necessary for the provision of health care. The custodian who receives the personal health information that has not been locked, may choose to explore the matter of the locked information with the individual. The custodian would need to obtain the express consent of that individual to access and use that locked information.

However, a custodian is permitted to disclose the locked information in certain circumstances, including to a recipient custodian where, in his/her professional opinion, the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to an individual or a group of persons.

Further, an individual's restriction may not impede a custodian from recording personal health information about an individual that is required by law, professional or institutional practice.

When does the lock-box provision take effect?

The lock-box provision came into force on November 1, 2004. Public hospitals have been granted a one-year extension, until November 1, 2005, to comply with an individual's express instruction not to use or disclose certain personal health information without consent.

What happens when an individual is incapable of providing consent?

PHIPA generally presumes that individuals are capable of making their own decisions regarding the collection, use or disclosure of their personal health information if they are able to understand and appreciate the consequences of providing, withholding or withdrawing their consent.

If a health information custodian believes that an individual is incapable of providing consent, *PHIPA* permits a substitute decision-maker (such as a relative, spouse, child's parent, or the Public Guardian and Trustee) to make a decision on an individual's behalf.

PHIPA lists, in order of priority, the following substitute decision-makers who may consent on behalf of an individual when consent is required, including:

- The guardian of the person or of the property;
- The attorney for personal care or property;
- The representative appointed by the Consent and Capacity Board;
- The spouse or partner;
- A child or parent (including the Children's Aid Society);
- A parent who has right of access;
- A sibling;
- A relative; and as a last resort
- The Public Guardian and Trustee.

Can another person, such as a family member, provide consent on an individual's behalf when picking up or dropping off a prescription?

Yes. The regulations permit a pharmacist to provide a prescription to another person unless the prescriber (a physician, for example) states otherwise. This is also permitted under the *Drug and Pharmacies Regulation Act*.

Collection, Use and Disclosure of Personal Health Information

Collection

What is a collection of personal health information under *PHIPA*?

PHIPA defines the term "collect" as the gathering, acquiring, receiving or obtaining of personal health information. This means that personal health information can be collected by a health information custodian or an authorized agent under *PHIPA* in several ways, such as when a doctor makes notes about a patient in his/her medical file or when a pharmacist fills a prescription.

What are the rules regarding the collection of personal health information?

Health information custodians within the circle of care may rely on an individual's implied consent to collect personal health information for the purpose of providing health care.

With limited exceptions, health information custodians must collect personal health information directly from the individual involved and may only collect as much information as is necessary to meet the purpose of the collection.

Custodians must take reasonable steps to inform the public about their information practices and how individuals may exercise their rights under *PHIPA*. Some suggested methods of meeting this requirement include the use of visible brochures, posters, notices posted on walls and verbal explanations.

What are the exceptions to the rules for collecting personal health information?

PHIPA provides for the collection of personal health information directly from individuals. Health information custodians may collect personal health information indirectly where, for example:

- The individual consents;
- The collection is necessary for providing health care and it is not possible to obtain the information directly from the individual in a timely manner;
- The custodian collects personal health information for the purposes of research from a person who is not a health information custodian, provided that certain conditions are met;

- The indirect collection is required or permitted by law;
- The indirect collection is required for the purpose of health planning or management; or
- The IPC authorizes the indirect collection.

Use

What is a use of personal health information under *PHIPA*?

"Use" of personal health information under *PHIPA* is defined as the handling or dealing with personal health information that is in the custody or control of a health information custodian or its authorized agent. This includes accessing or reproducing health information as required by the custodian.

What are the rules regarding the use of personal health information?

As a general rule, consent is required for any use of an individual's personal health information unless *PHIPA* allows the use without consent.

A health information custodian may rely on an individual's implied consent to share personal health information with its authorized agent, as long as the sharing is related to the provision of health care and the individual has not expressly stated otherwise.

When using personal health information, a custodian must exercise the highest level of care and must take reasonable steps to ensure that the individual's personal health information is as accurate, complete and up-to-date for the purpose which the custodian uses the information.

Where a health information custodian is authorized to use the information, the custodian may provide the information to an agent of the custodian to use it for that purpose on behalf of the custodian. The sharing of information between a custodian and its agent is considered to be a use and *not* a disclosure for the purposes of *PHIPA*.

What are the exceptions to the rules regarding the use of personal health information?

PHIPA sets out a limited set of acceptable uses of personal health information without consent, including for the following purposes:

- Risk management, error management, or activities to improve or maintain the quality of care or any related program or service;
- Educating agents to provide health care;
- The planning or delivering of programs or services;
- The allocation of resources to any program or service provided or funded by the custodian;
- Obtaining payment or processing, monitoring, verifying or reimbursing health care claims; and
- For research, provided that specific requirements and conditions are met.

A custodian may share personal health information with an agent of the custodian for any of these purposes.

Disclosure

What is a disclosure of personal health information under *PHIPA*?

The term "disclose" under *PHIPA* means to release or make available personal health information that is under the control or custody of a health information custodian, or its authorized agent, to another custodian, individual or organization. It does not include providing information directly back to the person who provided it in the first place, whether or not the information has been altered, so long as it does not include additional identifying information.

What are the rules regarding the disclosure of personal health information?

As a general rule, consent is required to disclose an individual's personal health information unless *PHIPA* allows the disclosure without consent.

A health information custodian and its authorized agents may rely on implied consent for the disclosure of personal health information within the circle of care while providing health care so long as the disclosure is reasonably necessary for the provision of health care and the individual has not expressly stated otherwise.

Although *PHIPA* permits custodians to disclose personal health information in certain limited situations, disclosure is not required, unless it is necessary to carry out a statutory or legal duty.

Express consent will always be required when personal health information is disclosed by a custodian to a non-custodian; where a custodian discloses to another custodian for a purpose other than for health care; or for marketing, research (unless specific conditions are met); and fundraising (if more than contact information is provided).

When disclosing personal health information, the custodian should take care to ensure that no information is inadvertently disclosed to third parties.

What are the exceptions to the rules regarding the disclosure of personal health information?

PHIPA recognizes the need for a flexible approach to regulating information exchanges between health information custodians in order to ensure the effective and efficient operation of the health system. As such, custodians may disclose personal health information without an individual's consent in certain circumstances, including the following:

- If the disclosure is reasonably necessary for providing health care and the consent cannot be obtained in a timely manner, unless there is an express request from the individual instructing otherwise;
- In order for the Minister of Health and Long-Term Care to provide funding to the custodian for the provision of health care services;
- For the purpose of contacting a relative or friend of an individual who is injured, incapacitated, ill or unable to give consent personally;
- To confirm that an individual is a patient or resident in a facility or to confirm the status of his/her health condition, unless there is an express request from the individual instructing otherwise;
- To identify an individual who is deceased or in order to allow a spouse, partner or relative of a deceased person to make decisions about his or her own care or the care of children or to inform estate trustees of an individual's death;
- To eliminate or reduce a significant risk of serious bodily harm to any person or the public;
- When transferring records to a custodian's successor or to the archives for conservation;
- For the purpose of carrying out an inspection, investigation or similar procedure that is authorized by a warrant, *PHIPA* or another *Act*;

- For determining or verifying eligibility for publicly funded health care or related benefits upon the request of the Minister of Health and Long-Term Care;
- For the purpose of administration and enforcement of various Acts by the professional Colleges and other regulatory bodies;
- To a prescribed "person" listed in the regulations that compiles and maintains a registry of personal health information for the purpose of improving the provision of health care or that relates to the storage or donation of body parts or bodily substances, namely:
  - Cardiac Care Network of Ontario (the registry of cardiac services);
  - INSCYTE (CytoBase);
  - London Health Sciences Centre (Ontario Joint Replacement Registry); and
  - Canadian Stroke Network (Canadian Stroke Registry);
- To a prescribed entity for the purpose of analysis or compiling information with respect to the management, evaluation or monitoring of the health system, including:
  - Cancer Care Ontario;
  - Canadian Institute for Health Information;
  - Institute for Clinical Evaluative Sciences; and
  - Pediatric Oncology Group of Ontario;
- To a health data institute for the purposes of health planning and management of the health care system;
- To the Public Guardian and Trustee, Children's Aid Society and the Children's Lawyer for the purpose of carrying out their statutory functions;
- To a person conducting an audit or reviewing an accreditation or application for accreditation related to the services of a custodian;
- To a medical officer or a public health authority as required for the purposes of the *Health Protection and Promotion Act*, for example, to report a communicable disease;
- For the purpose of legal proceedings if the information is, or relates to, a matter at issue;
- For the purpose of research, subject to restrictions and conditions; and
- For any purpose as required or permitted by law.

What is a health data institute?

PHIPA permits the Minister of Health and Long-Term Care to direct a health information custodian to disclose personal health information to an approved and secure health data institute. A health data institute is an independent organization authorized to receive personal health information from custodians for health care management and planning purposes.

Before a health information custodian releases personal health information to the health data institute, the minister must provide a comprehensive proposal for review and comment to the IPC. The institute may then release only de-identified information to the ministry, unless the IPC approves disclosure with minimal identifiers that is determined to be in the public interest.

In addition, the health data institute must comply with safeguards to respect the confidentiality of personal health information. In order to ensure compliance, the IPC will review and approve the practices and procedures of the institute every three years.

Can a health information custodian disclose personal health information to the Workplace Safety and Insurance Board (WSIB) about an injured worker without the individual's consent?

Yes. *PHIPA* permits the disclosure of personal health information without consent if permitted or required by another law. This means that *PHIPA* does not interfere with the *Workplace Safety and Insurance Act* where that Act requires a health practitioner to provide the injured worker, the employer and the WSIB information relating to an employee's health care or functional abilities. However, anyone relying on the disclosure provisions of another Act must be mindful that there may be further requirements with respect to the confidentiality of such reports.

Fundraising and Marketing

Can health information custodians collect, use or disclose personal health information for fundraising activities?

In general, custodians are only permitted to collect, use or disclose personal health information for non-health-care-related purposes with the express consent of the individual in question. However, *PHIPA* and the regulations provide special rules for fundraising. They provide that a collection, use or disclosure of an individual's name and mailing address (or the name and mailing address of a substitute decision-maker, if applicable) for fundraising may take place with the implied consent of the individual in question, as long as the following requirements are met:

- That the collection, use or disclosure of personal health information for fundraising purposes is only permitted where the fundraising relates to a charitable or philanthropic purpose related to the custodian's functions;
- That implied consent may only be inferred where the custodian has provided, or has made available, notice to the individual at the time an individual receives health care, informing that individual of the custodian's intention to use or disclose the information for fundraising purposes, along with information on how the individual can easily opt out;
- That the individual had not opted out within 60 days from the time the notice had been provided to him or her;
- That all solicitations contain an easy opt-out from any further solicitations; and
- That no solicitations contain information about an individual's health care or state of health.

Can personal health information be collected, used or disclosed for marketing purposes?

A health information custodian can only collect, use or disclose personal health information about an individual for market research or for marketing purposes with the express consent of the individual.

Note that the following activities are excluded from the definition of marketing:

- Blood donor recruitment by the Canadian Blood Services; and
- Communications by health care practitioners about the availability of non-OHIP covered charges for a block fee.

Research

What are the requirements for the collection, use and disclosure of personal health information for health care research?

In recognizing the importance of health research, *PHIPA* permits the use or disclosure of personal health information for research purposes without an individual's consent if strict conditions are met.

For example, a custodian who uses personal health information for research and, similarly, a researcher who seeks disclosure of personal health information for research, must both submit a detailed research plan to a Research Ethics Board (REB) for approval. In reviewing a research proposal involving the use and disclosure of personal health records, a REB must consider:

- Whether the research cannot be reasonably accomplished without access to the information;
- The public interest in conducting the research and in protecting privacy;
- Whether obtaining consent directly is impracticable; and
- Whether adequate safeguards are in place to protect the privacy of individuals and the confidentiality of their information.

A researcher requesting disclosure of personal health information from a custodian must submit to the custodian a written application, a research plan and a copy of the decision approving the research plan by the REB. In addition, the custodian must enter into an agreement with the researcher that may impose further restrictions on the manner in which the researcher may use and disclose the information.

A researcher with an approved research plan who receives personal health information from a custodian shall:

- Comply with the conditions imposed by the REB, if any;
- Use personal health information only for the purpose set out in the research plan;
- Not publish information in a form that could identify the individual;
- Not disclose information unless required by law or to prescribed entities or registries;

- Not attempt to contact the individual whose personal information is the subject of the research project unless the custodian obtains the consent of that individual; and
- Notify the custodian in writing of any breaches of either the agreement or *PHIPA*.

Researchers are permitted to disclose personal health information to another researcher or to a prescribed registry or entity if the disclosure is either part of a research plan approved by an REB or it is necessary for the purpose of verifying or validating the information held by the researcher.

Researchers who were in possession of personal health information and who lawfully obtained the information from a custodian prior to Nov. 1, 2004 may continue using and disclosing the information for three years after that date.

Are there any requirements for research ethics boards and research plans?

Yes. The regulations specify that a research ethics board (REB) must have at least five members, including:

- A member who has no affiliation to the person who established the REB;
- A member who has knowledge in privacy issues;
- A member who has knowledge in research ethics; and
- At least two members with expertise in the methods or the relevant areas of research.

In addition, the regulations list a number of requirements that research plans must include. For example, a research plan must include a description of why consent to the disclosure of personal health information is not being sought from the individual to whom the information relates; a description of how the information will be used; the safeguards the researcher will put in place to protect the confidentiality and security of the information; and a description of all persons who will have access to the information.

Ontario Health Cards and Health Numbers

Who can collect, use or disclose Ontario health card numbers and under what circumstances may this be disclosed?

Health information custodians and certain individuals or organizations prescribed in the regulations are permitted to collect, use or disclose Ontario health card numbers.

An individual or organization that is not a health information custodian may only collect or use an Ontario health card number for the following purposes:

- For the provision of publicly funded health services;
- For the purposes for which the custodian disclosed the number;
- For the regulation of health professionals; or
- For health administration, health planning, or health research or epidemiological studies by prescribed entities listed in the regulations including, the Workplace Safety and Insurance Board, Cancer Care Ontario, Canadian Institute for Health Information and the Institute for Clinical Evaluative Studies.

An organization or individual who is not a custodian may only disclose a health number for a number of limited purposes set out in the regulations or as authorized by law.

These restrictions on the collection, use and disclosure of health numbers do not apply to:

- A person who collects, uses or discloses health numbers for a proceeding;
- A prescribed entity set up to analyze the health care system; or
- A health data institute.

Are other organizations permitted to request the production of a health card?

PHIPA states that only individuals or organizations that provide provincially funded health care services may require the production of an individual's health card.

However, there is nothing in *PHIPA* that prevents an organization from requesting a health card, as long as it is made clear that disclosure is voluntary, and the information will only be used for the purpose of providing health care services.

For instance, an employer may allow an employee to voluntarily provide his or her health card in order to expedite the provision of health care services in the event of an emergency.

Please note that any such disclosure must be voluntary, and non-custodians may not require the production of health cards. It is an offence under *PHIPA* for any organization to wilfully collect, use or disclose any personal health information – including health card numbers – in a manner that contravenes *PHIPA*.

Likewise, an individual may voluntarily provide his/her health card to a library in order to confirm his/her identity and in order to obtain a library card.

Access to Personal Health Information

Are individuals permitted to access their own personal health information?

With limited exceptions, *PHIPA* provides individuals with a general right to access their own personal health information held by a health information custodian and sets out a formal procedure for access requests. The right of access does not apply to records that contain quality of care information, information required for quality assurance programs, raw data from psychological tests or assessments, information used solely for research purposes, and to some information in the custody or control of a laboratory where an individual has the right of access to that information from his/her health information custodian.

How does an individual obtain access to his/her personal health information?

An individual may request access to his/her own personal health information by formally submitting a written request to the health information custodian who has custody or control of the individual's health records. An individual may also request his/her personal health information orally. Whether the access request is made orally or in writing, the request must contain sufficient detail to allow the custodian to locate the record in question.

The health information custodian should then either provide access to or a copy of the record. Otherwise, a written notice explaining why the record is not available must be provided to the individual seeking access.

Where the individual has not provided sufficient detail to enable the custodian to identify and locate the record, the custodian is required to assist the individual in reformulating the request.

How long does a health information custodian have to respond to an individual's request for access to personal health information?

A health information custodian must respond no later than 30 days after the request was made.

Extensions beyond this 30-day time frame are allowed where meeting this time frame would interfere with the custodian's operations, or where outside consultations are required in order to comply with the request. In such situations, the custodian must inform the individual in writing about the delay and the reasons for the delay.

Can a health information custodian refuse to provide access to an individual's personal health information?

Generally, health information custodians are responsible for assisting individuals by providing access to their health records.

Custodians may only refuse access in limited situations, including:

- The information in question is subject to a legal privilege;
- Its disclosure could reasonably be expected to result in a risk of serious bodily harm to a person;
- The information was collected as part of an investigation; or
- Another law prohibits the disclosure of that information.

If any exception applies, *PHIPA* permits custodians to remove some of the information to allow partial access to the individual. If a health information custodian denies an individual access to his/her personal health information, the individual has the right to file a complaint with the IPC.

Is there a fee associated with an access request?

Health information custodians may charge a reasonable fee for providing access to an individual's personal health records. *PHIPA* also permits a custodian to waive all or part of the fee associated with an access request.

In charging a fee, *PHIPA* requires custodians to provide the individual with a fee estimate limited to the prescribed amount set out in the regulations, if any, or an amount that is reasonable for cost recovery.

Can an individual obtain access to his/her personal health information from a health information custodian who works for a non-health information custodian?

Yes, if the non-health information custodian is not covered by public sector access and privacy legislation. The request would be made directly to the health information custodian.

What if the health information custodian works for a non-health information custodian that is covered under public sector access and privacy legislation, such as a school board or municipality?

In that case, the individual would submit an access request under the *Freedom of Information and Protection of Privacy Act* (which covers provincial ministries and most provincial boards, agencies and commissions) or the *Municipal Freedom of Information and Protection of Privacy Act* (which covers local government organizations such as municipalities, police, school, health and library boards) directly to the freedom of information co-ordinator of the non-health information custodian. This does not mean, however, that an individual cannot make an access request directly to the health information custodian, who presumably, would take the necessary administrative steps to obtain it from the freedom of information co-ordinator.

Corrections to Personal Health Information

Can an individual correct errors in his/her personal health information?

An individual who believes that his/her personal health information is incomplete or inaccurate may request that a health information custodian correct his/her record. It is the responsibility of the custodian to ensure that personal health information is complete and accurate.

How does an individual correct errors?

An individual seeking a correction to his/her personal health information is required to submit a written request to the health information custodian who has custody or control of the records. The custodian must respond within 30 days of receiving a correction request.

PHIPA provides limited grounds for extending this 30-day time frame. Specifically, extensions are permitted where replying within 30 days would unreasonably interfere with the custodian's activities, or where the time necessary to undertake the consultations associated with the request would exceed 30 days.

Can a health information custodian refuse to correct an individual's personal health information?

A health information custodian is obligated to correct personal health information where an individual demonstrates, to the satisfaction of the custodian, that the record is in fact inaccurate or incomplete and the individual gives the custodian the necessary information to correct the record.

However, a custodian may refuse to correct personal health information that was not created by the custodian or that is a professional opinion or an observation of a health care provider. If a correction is refused on such a basis, the custodian is required to inform the individual of the refusal, the reasons for the refusal, the individual's right to file a complaint regarding the refusal to the IPC and the right of the individual to attach a statement of disagreement to the record.

Administration and Enforcement

How will *PHIPA* be enforced?

The IPC has been designated as the independent oversight body responsible for ensuring that health information custodians collect, use and disclose personal health information according to the rules set out under *PHIPA*. The IPC will play a significant role in enforcing overall compliance.

The IPC has various powers under *PHIPA*, including the authority to investigate and adjudicate complaints. These include the authority to:

- Require a complainant to try to resolve the issue directly with the custodian;
- Investigate a complaint initiated by an individual or in the absence of a complaint, self-initiate reviews; and
- Appoint a mediator to resolve the complaint.

The IPC also has the authority to issue orders requiring compliance with *PHIPA*. For example, the IPC may order a custodian to:

- Provide the individual with access to a record of personal health information;
- Correct a record of personal health information;
- Dispose of records of personal health information; and
- Change or cease a particular information practice.

How does an individual initiate a complaint?

An individual who feels that his/her privacy rights under *PHIPA* have been violated has the right to submit a written complaint to the IPC. For example, an individual may complain about:

- A health information custodian's information practices;
- A refusal to grant access to his/her personal health information; or
- A refusal to correct or amend his/her personal health information.

Is there a time limit within which an individual may complain?

In general, an individual must file a complaint with the IPC within one year from when the individual became aware of the problem. The legislation provides the IPC with the discretion to extend this one-year limitation period.

For complaints that deal with access or correction, an individual must file a complaint with the IPC within six months from the time a health information custodian refuses an access or correction request.

If an individual is not satisfied with an IPC order, what can be done?

An individual who is not satisfied with an order issued by the IPC has the right to appeal the decision on a question of law to the Divisional Court of Ontario within 30 days of receiving a copy of the order. Where the IPC issues an order relating to access or correction of health records, there is no right of appeal. In such a case, an individual may apply to the Divisional Court for judicial review.

Where the IPC issues a final order relating to a health information custodian under *PHIPA*, a complainant has the right to pursue a remedy in court for any harm suffered as a result of a privacy breach. In addition, if a court determines that the harm suffered by the complainant was caused by the wilful or reckless misconduct of a health information custodian, *PHIPA* permits the court to award up to $10,000 in damages for any mental anguish suffered.

What are the consequences for committing an offence under *PHIPA*?

An individual found guilty of committing an offence under *PHIPA* can be liable for a fine of up to $50,000. An organization or institution can be liable for a fine of up to $250,000.

Any officer, member, employee or agent of a corporation found to have authorized or acquiesced to a breach of *PHIPA* can be held personally liable.

In addition, health information custodians who are convicted of an offence under *PHIPA* may be subject to a civil suit for damages. Generally, health information custodians who have acted reasonably and in good faith will be protected from liability.

What is an offence under *PHIPA*?

Offences under *PHIPA* include:

- Wilfully collecting, using or disclosing personal health information in contravention of *PHIPA*;
- Obtaining or attempting to obtain health information under false pretenses;
- Knowingly disposing of health records to avoid providing access;
- Misusing Ontario health card numbers;
- Obstructing the IPC or one of its delegates in the performance of its oversight functions;
- Disciplining or harassing an individual who has alerted the IPC of an alleged contravention; or
- Failing to comply with an IPC order.

The *Quality of Care Information Protection Act, 2004*

What is the *Quality of Care Information Protection Act, 2004* (*QOCIPA*)?

QOCIPA was designed to assist in reducing medical errors and thereby improving patient safety in hospitals. Personal health information, collected by a designated "quality of care committee" under *QOCIPA*, that contains information relating to an adverse event, such as a patient death or prolonged injury or illness due to a medical error, may not be disclosed for the purposes of litigation and may not be accessed by a patient.

QOCIPA defines a "quality of care committee" as a facility that conducts quality of care and peer review activities. "Quality of care information" is defined as information collected by a quality of care committee for the purpose of carrying out these activities.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca